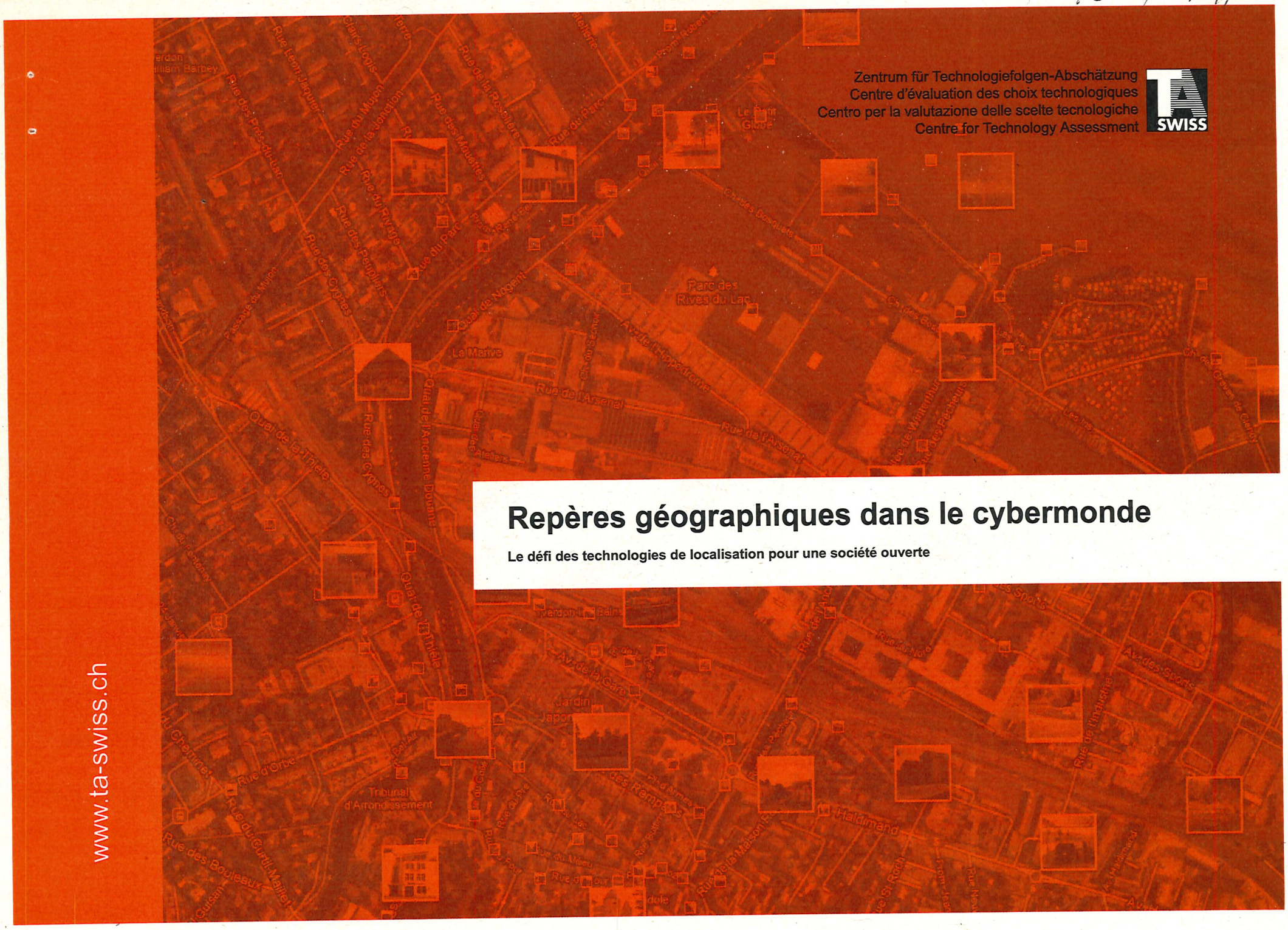

Zentrum für Technologiefolgen-Abschätzung
Centre d'évaluation des choix technologiques
Centro per la valutazione delle scelte tecnologiche
Centre for Technology Assessment
TA SWISS
Repères géographiques dans le cybermonde
Le défi des technologies de localisation pour une société ouverte
www.ta-swiss.ch

Informations sur l'étude «Lokalisiert und identifiziert. Wie Ortungstechnologien unser Leben verändern»

L'étude a été réalisée avec le soutien de l'Office fédéral de la statistique OFS, de l'Office fédéral des routes OFROU et de l'Office fédéral de topographie swisstopo.

Lorenz Hilty, Britta Oertel, Michaela Wölk, Kurt Pärli

Lokalisiert und identifiziert
Wie Ortungstechnologien unser Leben verändern

TA-SWISS, Centre d'évaluation des choix technologiques (éd.). vdf Hochschulverlag AG der ETH Zürich, 2012.

ISBN 978-3-7281-3460-8

Aussi disponible en open access:
www.vdf.ethz.ch/info/showDetails.asp?isbnNr=3460

Résumé disponible en ligne: www.ta-swiss.ch

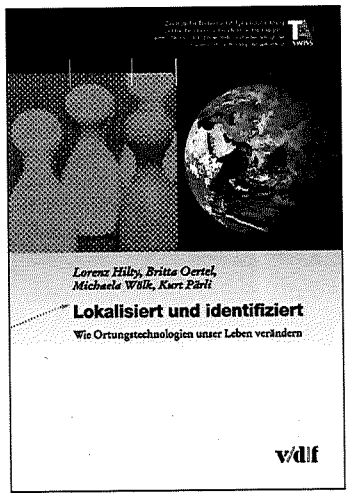


Table des matières

La localisation en bref 4

1 Géodonnées au passage entre cybermonde et réalité 5
Classement et espionnage également facilités 5
Le parcours fouineur du cyberharceleur 5
Diverses formes de techniques de localisation 6

2 Des techniques de localisation pour chaque usage 7
Au service de la mobilité 7
Culture de l'amitié dans les réseaux sociaux 7
Mettre en balance sécurité et liberté 8
Tutelle ou autonomie ? 8
Où suis-je – et où sont mes données ? 9

3 Protéger ses données personnelles 10
Perte de contrôle garantie 10
S'abstenir n'est pas non plus une solution 11
Le détournement des objectifs est juridiquement discutable 11
Nombreuses lacunes au niveau de la mise en œuvre 11
La globalisation des communications nécessite une protection mondiale 11

Etude «Technologies de localisation» 13

Impressum 14

La localisation en bref

Pour être en réseau avec le monde entier, plus besoin d'être assis devant son ordinateur ou à côté du téléphone: l'ordinateur portable et le téléphone mobile permettent de ce connecter à internet et de mener partout des conversations téléphoniques. Ce faisant, nous laissons des traces, qui peuvent servir à reconstituer nos déplacements: les opérateurs de téléphonie mobile savent quand et à quelle antenne nous nous sommes enregistrés, et les fournisseurs de services internet connaissent notre adresse IP, qui permet de déduire approximativement le lieu où nous nous trouvons. Lorsque nous naviguons sur internet en recourant à la radiocommunication à courte portée (WLAN), la localisation est même assez précise. Toujours plus d'objets d'usage quotidien sont munis de fonctions de localisation.

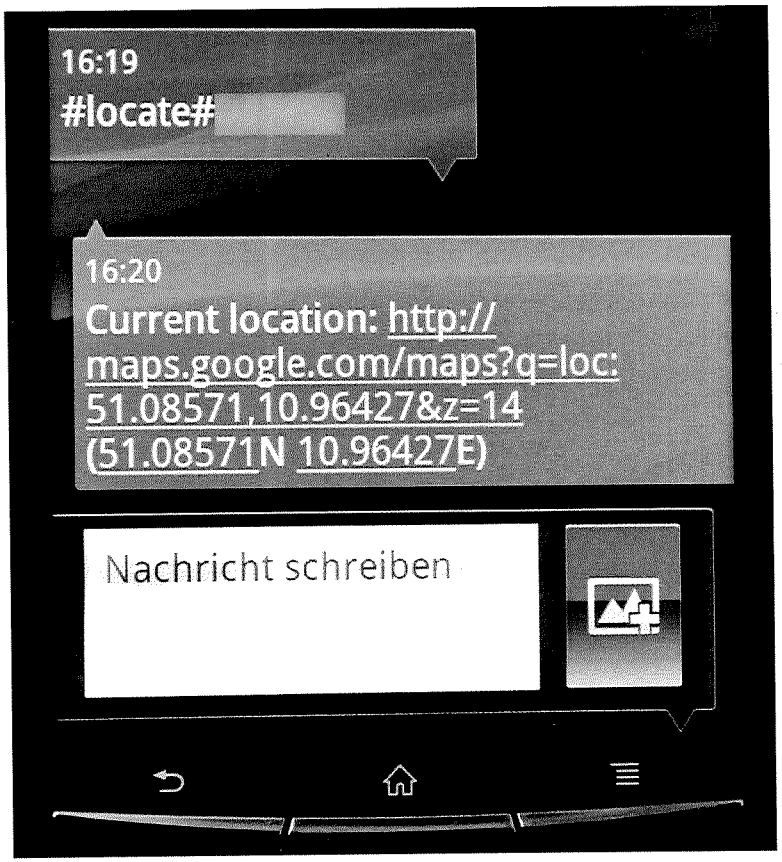
C'est pourquoi les données de localisation servent de plus en plus de base à des modèles commerciaux et prestations innovantes. Des indications sur la position en temps réel peuvent aider des services de sauvetage à trouver rapidement les sinistrés. Et l'enregistrement de profils de déplacement est utile à la planification du trafic pour déceler et éliminer des goulets d'étranglement sur les routes. L'exploitation de données de localisation recèle cependant aussi des risques. Qui fournit trop ouvertement des informations géolocalisées expose sa vie et ses habitudes à des regards indiscrets. De plus, des réseaux sociaux tels que Facebook ont coutume de transmettre de nombreuses informations personnelles à des tiers intéressés aux données de localisation à des fins de marketing, si bien que celles-ci se propagent par des voies opaques à l'insu des personnes concernées.

Par son étude «Lokalisiert und identifiziert. Wie Ortungstechnologien unser Leben verändern», TA-SWISS veut faire prendre conscience de cette problématique et suggérer des recommandations sur la manière d'utiliser les données géolocalisées.

Recommandations tirées de l'étude de TA-SWISS

Les décisionnaires du monde politique et de l'administration sont concernés à plusieurs égards:

- Ils doivent soutenir des mesures permettant d'imposer la protection des données au niveau international.
- Les systèmes de localisation doivent être intégrés au «Programme suisse pour la protection des infrastructures critiques» dans la mesure où l'organisation de services de sauvetage, de systèmes de transport et d'autres champs d'action de la main publique tire parti de ces technologies.
- Il faut que des logiciels dont la fiabilité et la transparence sont attestées, reçoivent une certification, pour faire de la protection des données une marque de qualité de ces produits.
- Il faut inscrire dans la loi une limite de la durée de conservation des données de localisation; les personnes concernées devraient se voir remettre une sorte de «gomme numérique» leur permettant d'imposer leur droit à l'oubli à l'égard des données de localisation les concernant.
- Des recherches empiriques supplémentaires sont nécessaires en sciences sociales pour combler des lacunes du savoir en rapport avec les données de localisation.
- Enfin, les compétences en matière de médias électroniques doivent être améliorées, de façon générale, et en particulier auprès des jeunes, pour sensibiliser ceux-ci aux atouts et risques résultant de la mise en ligne de leurs profils de déplacement et lieux de séjour.



La présente synthèse repose sur l'étude intitulée «Lokalisiert und identifiziert. Wie Ortungstechnologien unser Leben verändern» (Localisé et identifié. Comment les technologies de localisation changent notre vie). Elle a été réalisée par une équipe interdisciplinaire sous la direction de Lorenz Hilty, de l'EMPA (www.ta-swiss.ch).

1 Géodonnées au passage entre cybermonde et réalité

L'alibi tranche souvent entre condamnation et acquittement. Non sans raison: traduit, ce mot signifie «ailleurs», c'est-à-dire «pas sur le lieu du crime». En effet, des informations sur le lieu où une personne se tient, permettent de tirer des conclusions sur ce qu'elle fait, perçoit et sait. L'accès à des données au sujet de qui se tient à un moment donné en un lieu bien défini ouvre donc de nombreuses possibilités – en bien comme en mal.

«Ouah! c'est où ça?», poste le 15 mars 2010 un internaute qui regarde la collection de photos numériques de Jean-Frédéric Beaudet. La prise de vue a beaucoup d'atmosphère et montre un entrepôt abandonné sur lequel le temps semble peser lourdement. Seule la lumière chaude qui éclaire ce lieu fait que les étagères empoussiérées et les supports d'acier rouillés suscitent la nostalgie plutôt que l'angoisse. En fait, le visiteur du portail de photos Picasa de Google n'aurait pas eu besoin de poser la question du lieu. Car ses coordonnées figurent sur le bord droit de l'image: 46,755165 degrés de latitude nord et 71,290497 de longitude ouest. Google Maps attribue cette position à une zone industrielle et artisanale désaffectée à la périphérie de Saint Louis, une subdivision administrative de la ville de Québec au Canada. Grâce à Google Street View, l'entrepôt abandonné peut même être vu de l'extérieur; l'édifice blanc barbouillé de graffitis est nettement moins pittoresque qu'on ne l'aurait supposé en voyant l'intérieur.

Les données associées à l'image révèlent aussi qu'un Canon EOS Digital Rebel XTi a été utilisé pour la photo – un modèle muni d'un récepteur GPS (Global Positioning System) et capable d'enregistrer automatiquement des informations sur le lieu de la prise de vue. Toujours plus d'appareils photo numériques et de caméscopes sont équipés de récepteurs GPS. Mais grâce à un tracker GPS séparé, raccordé de l'extérieur à l'appareil photo, personne ne doit renoncer aux géomarques, même s'il utilise un ancien modèle. Et lorsque quelqu'un photographie ou filme au moyen d'un smartphone de nouvelle génération, l'appareil assigne par défaut les données de localisation aux prises de vue; si cette application est fermée, d'autres apps cessent aussi souvent de fonctionner.

Classement et espionnage également facilités

Nombre d'utilisateurs de portails photo tels que Picasa, Flickr, Fotocommunity ou Locr apprécient l'indication complémentaire de la position, car des photos publiées en ligne peuvent alors faire l'objet d'une recherche en fonction du lieu de la prise de vue. Le portail Panoramio utilise même des données géographiques comme principe de classement de sa collection. Cela ne pose pas problème pour des paysages ou des reflets de l'atmosphère d'une ville. En revanche, des instantanés pris lors d'un anniversaire, d'une noce ou d'autres événements privés peuvent laisser des traces brûlantes permettant à des indiscrets d'espionner la vie des personnes photographiées.

L'exemple d'une jeune famille, dont certaines activités ont été mises en ligne, illustre bien la situation. Salomé et Klemens Christen-Kaiser se sont mariés au début de l'automne 2006; la photo publiée sur une plate-forme web les montre le jour de leur mariage civil avec leur fille Gianna dans le chef-lieu de leur canton de domicile, devant l'office de contrôle des habitants. Avec ses yeux foncés et ses cheveux bruns, la petite tient beaucoup de sa maman; elle n'a en tout cas rien des boucles blondes de son père. La collection de photos révèle aussi que Gianna est venue au monde huit mois avant le mariage: des images la montrent comme bébé habillé d'une brassière jaune pâle.

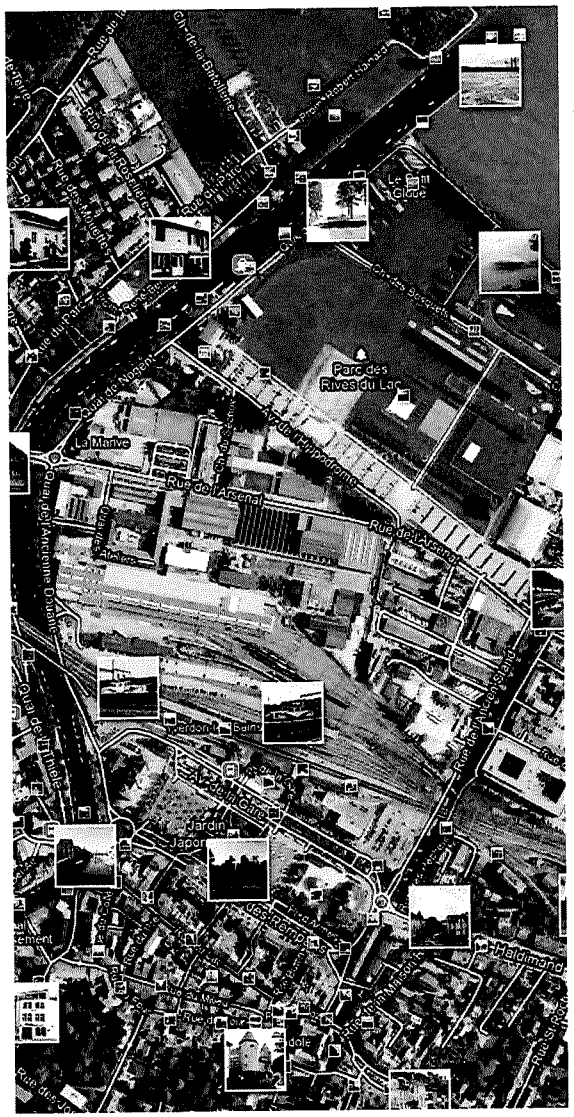
Le parcours fouineur du cyberharceleur

La collection de photos publiée sur internet révèle beaucoup de choses sur la famille Christen. C'est Patrick Siegenthaler, parrain de Gianna et ami de longue date de Klemens, qui les a rassemblées. Une photo de classe du début des années 1990 prouve qu'ils étaient ensemble à l'école secondaire. Que quinze ans plus tard le confiseur renonce à l'habituel glaçage blanc sur le gâteau de mariage du jeune couple passe comme simple anecdote; mais le fait que Klemens soit un excellent sportif touche déjà davantage à la sphère privée. Il a belle allure à Saas Fee sur son snowboard. On le voit aussi participant à diverses randonnées, par exemple au Parc national suisse («pris à Tarasp, canton des Grisons, Suisse» indique le texte commentant la photo), ou encore lors d'un tour à vélo dans l'Ouest de la France («pris à Grayan-et-l'Hôpital, Aquitaine, France»). Un fait instructif est que Salomé et Klemens ont choisi un «arbre à souhaits» pour Gianna dans un grand parc de leur ville et qu'ils y photographient régulièrement leur fille; quiconque scrute la collection de Patrick en fonction de ce lieu trouve une série d'instantanés qui documentent le développement de l'enfant, du bébé joufflu à la petite fille à la coiffure rigolote.

En publiant ses photos, Patrick n'agit même pas de façon indiscrète: les noms de famille de Klemens et Salomé ne figurent dans aucune légende. Ce sont des photos de divers événements sportifs – des marathons, des courses de vélos et de skis – qui sont en fin de compte divulgatrices. Plusieurs d'entre elles montrent le couple comme membre d'un team; or le site web de l'événement publie les photos des équipes avec nom et prénom des participants.

Il est alors aisé, dans l'étape suivante, d'obtenir encore davantage de détails en se référant à des réseaux sociaux tels que Facebook, LinkedIn ou Xing: Salomé est biologiste de l'évolution, et pendant ses loisirs, elle aime bien, entre autres, casser du bois; Klemens est employé dans une société d'informatique. Les portraits sur le site web de l'employeur confirment qu'il s'agit bien d'eux, et non pas de personnes qui auraient par hasard le même nom. A noter que dans le présent rapport les noms des personnes décrites ont été modifiés et les lieux indiqués sur les photos laissés en partie dans le vague. Mais le cas est réel et la leçon claire: qui publie des données personnelles sur internet doit compter que des indiscrets découvrent des détails sur sa biographie, ses relations et ses habitudes. Quiconque «gazouille» de surcroît régulièrement sur Twitter, comme le fait Salomé, ouvre sans le vouloir encore d'autres fenêtres sur sa vie privée: ses sympathies politiques se manifestent, ses préférences – ou encore l'utilisation régulière d'une liaison ferroviaire donnée.

Les informations sur des trajets fréquemment parcourus sont particulièrement instructives, car chez l'être humain, l'habitude est une seconde nature. Selon des études, un fouinard qui parvient à dépister le profil de déplacement d'une personne pendant trois mois est en mesure de prédire avec un taux de succès de 93 pour-cent le lieu où elle se trouve à un moment quelconque. Des données indiquant où quelqu'un habite ou se tient volontiers sont aussi éloquentes. Car que les photos de vacances aient été prises à Dubaï ou à Engelberg, et que l'on fréquente l'auberge de jeunesse ou l'hôtel cinq étoiles, est révélateur de la situation financière. Et bien que la famille Christen renonce sciemment à son inscription dans l'annuaire téléphonique, un peu de talent combinatoire permet d'identifier sa commune de domicile. Grâce à des services tels que Google Earth ou Street View, on a vite fait de constater, sans se rendre sur place, si le domicile est situé dans un quartier de villas, un village de paysans ou un quartier d'immeubles-tours.



Diverses formes de techniques de localisation

- Localisation par satellites, Global Positioning System (GPS): Développée à l'origine pour la navigation dans le secteur militaire, elle est utilisée aujourd'hui dans les domaines les plus divers. En plein air, les récepteurs GPS déterminent la position avec une précision d'environ 10 mètres (sauf dans les zones d'ombre formées par des bâtiments ou des tunnels).
- Téléphone mobile: La localisation a lieu par le biais des antennes de téléphonie mobile. La précision des données de localisation dépend notamment de la densité des mâts d'émetteurs; dans les agglomérations urbaines, son ordre de grandeur est d'une centaine de mètres si les conditions sont favorables. L'appareil est identifié par sa carte SIM. En outre, des modèles techniquement avancés avec accès à internet, les smartphones, sont équipés d'un module GPS qui permet une localisation plus précise; la plupart des téléphones mobiles vendus en Suisse sont des smartphones.
- Les WLAN (Wireless Local Area Networks, réseaux locaux radioélectriques) permettent à des ordinateurs proches les uns des autres de communiquer sans fil entre eux et avec internet. Une station WLAN de base procure l'accès sans fil à un réseau local. Les appareils portables sont localisés par rapport aux stations de base pour autant que celles-ci soient enregistrées dans des banques de données corrélatives.
- Localisation par l'adresse IP: Pour accéder à internet, chaque appareil a besoin d'une adresse IP. Les opérateurs octroient des adresses IP dynamiques aux terminaux au moment où ils sont actifs. Vu que chaque opérateur a un stock fixe d'adresses à disposition qu'il peut attribuer, la connaissance de l'adresse IP permet d'établir la position géographique d'un terminal dans les limites d'une certaine zone. La localisation exacte présuppose que l'opérateur livre les données de la connexion.

2 Des techniques de localisation pour chaque usage

Les satellites du GPS (Global Positioning System) ont été mis sur orbite dans les années 1970 par l'armée américaine spécialement pour la détermination de positions et la mesure du temps. Ce système est le moyen le plus connu, mais pas le seul, de localiser des personnes et des appareils. Le WLAN, largement utilisé, de même que les adresses internet d'ordinateurs et bien sûr aussi de smartphones, trahissent également le lieu où l'on se trouve.

Klemens et Salomé se déplacent beaucoup à vélo et utilisent souvent le train et le tram – ceci aussi est attesté par des photos et des blogs. Il est donc probable qu'ils consultent également les horaires et informations de voyage que les sociétés de transport mettent à disposition sur les téléphones mobiles – en partie exactement en fonction de la localisation du smartphone.

Au service de la mobilité

Les techniques de localisation facilitent aussi pour la famille Christen-Kaiser l'organisation d'excursions dans un rayon plus étendu, qui nécessitent différents moyens de transport et le franchissement de limites tarifaires: plus besoin pour cela de se rendre à l'automate à billets, il suffit de prendre avec soi son téléphone mobile sur lequel le titre de transport électronique a été chargé sous la forme d'un code barre. Un projet lancé il y a quelques années en Suisse sous le nom d'«ETIK», qui se trouve au stade du développement, pousse les commodités encore plus loin. Avec ETIK, on n'a même plus besoin de connaître à l'avance la destination d'une excursion. Un capteur inséré dans une petite carte en matière synthétique enregistre sans contact les voyageurs à leur entrée dans un véhicule et à leur sortie. Les lieux d'entrée et de sortie, l'heure, la classe du wagon et d'autres données nécessaires au paiement sont saisies, enregistrées dans le véhicule même et transmises à un serveur à la fermeture du service. Une condition est que les véhicules soient équipés du GPS, pour que leur localisation soit à tout instant bien établie. Un procédé de prépaiement se prêterait aussi bien pour encaisser le prix du billet que la facturation ultérieure, et un affinement de la structure du tarif n'est pas exclu à plus longue échéance: des rabais flexibles pourraient être accordés aux voyageurs circulant pendant les heures creuses; et il serait possible de changer de classe spontanément et sans tracas. En outre, des offres plus étendues pourraient être intégrées au billet électronique, par exemple l'entrée dans un musée ou l'utilisation de téléskis. A noter qu'ETIK ne produit pas de profils de déplacement: les données sont rendues anonymes et effacées après un délai fixé.

En tant que fervent adepte des sports d'hiver, Klemens peut tirer parti du développement des appareils d'aide à la recherche des victimes d'avalanche. Les modèles de la nouvelle génération sont munis, en plus de l'habituel radar, de récepteurs GPS et fournissent ainsi des informations supplémentaires pour la localisation rapide des personnes enfouies sous la neige, notamment hors des pistes. En été, la fonction de recherche en cas d'avalanche peut être inactivée et l'appareil utilisé pour s'orienter. Il enregistre l'itinéraire suivi, lequel peut ensuite être chargé sur un ordinateur et partagé avec d'autres cyclistes ou randonneurs.

Avec leurs iPhones, Klemens et Salomé peuvent en outre bénéficier d'une application développée par la garde aérienne suisse de sauvetage (Rega). Lors d'un appel d'urgence, cette app transmet des données précisant le lieu où se trouve l'appelant et accélère ainsi la recherche – un gain de temps qui peut sauver des vies. Le système d'appel d'urgence eCall, dont l'UE prévoit l'introduction pour le trafic routier, est aussi basé sur le GPS et des modules de téléphonie mobile. L'idée: en cas d'accident, un appareil de contrôle déclenche un appel d'urgence; simultanément, les systèmes de localisation sont activés. Aucun profil de déplacement n'est produit, mais le service de sauvetage reçoit néanmoins les coordonnées qui lui permettent d'intervenir rapidement. A partir de 2015, les nouvelles voitures devront être équipées de ce nouveau système; on en attend de grands avantages dans les cas où les victimes ne sont plus en mesure de communiquer avec la centrale d'appels d'urgence ou que des touristes ne maîtrisent pas la langue du pays.

Les données géographiques ne sont pas les seules informations révélatrices sur des personnes. La «surveillance d'essaims» procure des avantages notamment à la gestion du trafic routier: si de nombreux téléphones mobiles avancent au pas sur une autoroute, c'est qu'il y a un bouchon. De telles données de mouvement ne servent pas seulement à l'alerte en cas d'embouteillages, mais peuvent être utiles aussi à la planification du trafic, pour organiser l'espace routier en fonction des besoins.

Enfin, des techniques de localisation peuvent contribuer à optimiser aussi des trajets à l'intérieur d'un bâtiment. Des hôpitaux se servent par exemple d'une app développée en ce sens à la Haute Ecole de Bingen, en Allemagne. En cas d'appel d'urgence, elle alarme par WLAN uniquement les médecins qui se trouvent dans un certain rayon autour de l'incident, affaire d'économiser du temps et d'éviter de l'agitation.

Culture de l'amitié dans les réseaux sociaux

Les données de localisation ont suscité récemment des discussions en relation avec les réseaux sociaux. Nombre d'entre eux, tels que les classiques Facebook, Google+ ou Twitter, offrent aussi une fonction de localisation sur leurs apps pour téléphone mobile. Des

plates-formes de communication plus jeunes, comme Foursquare ou Yelp, ont même été conçues spécialement pour une utilisation en référence à un lieu. Cela permet à l'utilisateur, qui a préalablement mentionné sa position sur une carte interactive, de regarder quels «amis» se trouvent au voisinage. Il s'agit en général d'une autolocalisation; cela signifie que l'utilisateur fait lui-même connaître sa position, par exemple en entrant un lieu donné.

Dans le cas de Twitter, qui limite la longueur des messages, l'adjonction de la fonction de localisation est un véritable plus – aucun des 140 signes à disposition ne doit être sacrifié pour donner une information géographique. Cette fonction n'est pas en service par défaut, mais doit être activée par les utilisatrices et utilisateurs, qui peuvent décider en outre chaque fois qu'ils entrent un texte s'ils veulent divulguer ou non le lieu où ils se trouvent. En dépit de cette approche comparativement exemplaire des données de position, les spécialistes mettent en garde les «gazouilleurs» assidus contre les dangers auxquels ils s'exposent. Qui envoie fréquemment des annonces de statut et publie de surcroît ses données de position en cours de route révèle à d'éventuels cambrioleurs quand son appartement est inoccupé.

Les réseaux sociaux sont vantés par leurs créateurs comme des plates-formes d'échange privé entre personnes ayant des intérêts communs; cependant, ils ne sont pas moins intéressants pour l'économie. Le service allemand «friendticker», gratuit pour les utilisateurs privés, prélève auprès des entreprises un droit d'inscription et une taxe supplémentaire pour chaque enregistrement réussi d'un nouveau membre. En acceptant les conditions générales, les membres consentent en outre à ce que de la publicité soit envoyée sur leur écran. Les données de position rendent possible un micromarketing focalisé sur un lieu donné, incluant de la publicité taillée sur mesure en fonction des intérêts du propriétaire du téléphone mobile. C'est ainsi que Salomé pourrait recevoir un jour sur l'écran de son mobile mention du restaurant végétarien situé à deux pas ou du magasin d'articles de sport en plein air le plus proche.

Mettre en balance sécurité et liberté

Un spécialiste des TI comme Klemens connaît plusieurs moyens de tirer parti des techniques de localisation au cas où quelqu'un volerait son ordinateur portable. Des programmes spécifiques peuvent être installés à cette fin sur l'appareil. Si celui-ci disparaît, son propriétaire se connecte à un site web, y remet un avis de disparition et demande les données de position du portable. Dès que celui-ci est allumé, il transmet sa position, qu'il détermine grâce au WLAN ou – de façon moins précise – par l'adresse IP. Les médias relatent des cas où la personne victime du vol a pris une photo du larron au moyen de la caméra du portable et l'a publiée ensuite sur Facebook; cette chasse privée au voleur aurait été couronnée de succès. Des apps existent également pour les téléphones mobiles, grâce auxquelles un appareil volé ou perdu peut être localisé.

Pour augmenter la sécurité dans les passages souterrains, les halls de gare ou les transports en commun, les autorités et entreprises misent toujours plus fréquemment sur des caméras vidéo. Le recours à ces dernières peut en effet renforcer le sentiment de sécurité des passantes et passants. Nombre de conducteurs de trams et de bus apprécient aussi ces caméras comme protection en cas de bagarres ou d'autres incidents. Des études attestent que la vidéosurveillance contribue, particulièrement dans les transports publics, à prévenir les actes de violence et de vandalisme. Mais dans ce cas aussi, il y a production de données géographiques de position, vu que des personnes sont filmées en des lieux déterminés – souvent sans qu'elles en soient conscientes.

La sécurité est également une préoccupation de premier plan pour les systèmes de surveillance de personnes. Un exemple connu est le recours aux entraves électroniques dans le système pénal. La loi sur la police de certains cantons, par exemple de Bâle-Campagne, autorise l'utilisation d'entraves électroniques munies d'un système GPS quand il s'agit de protéger des personnes vis-à-vis de partenaires violents ou de harceleurs. Grâce aux données transmises par le système, les autorités voient si l'individu surveillé respecte l'interdiction de périmètre qui a été décrétée. Un espace de protection, que le stalker n'est pas autorisé à pénétrer, est ainsi tendu tout autour de la personne menacée.

Tutelle ou autonomie ?

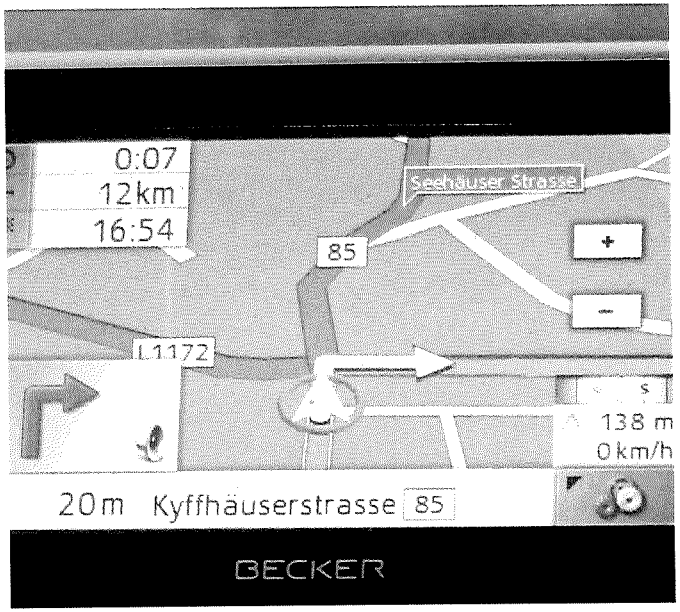
Les barrières de protection électroniques peuvent être aussi conçues de manière à empêcher les protégés de quitter un espace donné. De tels systèmes de surveillance ont fait des vagues dans des écoles US-américaines et britanniques. La direction de l'école n'utilisait pas seulement les données de position pour contrôler la présence des élèves pendant l'enseignement, mais autorisait le fournisseur à se servir des informations pour la promotion de son système. De nombreux parents ont été choqués par cette exploitation subsidiaire des données qui n'était ni contrôlée ni transparente. Enfin, une barrière virtuelle de protection peut être installée pour déclencher une alarme lorsque des personnes à risque – par exemple des patients Alzheimer – quittent une zone définie. Dans ce cas, un bracelet muni d'une fonction de localisation permet d'élargir le rayon de déplacement des personnes concernées, qui devraient sinon être confinées sur le terrain de la clinique par des barrières réelles. Néanmoins, le dilemme est programmé

d'avance quand il s'agit de décider entre répondre au besoin de sécurité et satisfaire l'aspiration à la liberté. Quand on a affaire à des personnes qui ne sont pas en mesure d'articuler elles-mêmes leurs intérêts et de mesurer la portée de leurs décisions, il faut être particulièrement attentif à mettre soigneusement en balance assistance et autonomie Que l'Etat dispose des moyens pour surveiller des individus – par exemple dans la lutte contre la criminalité – est dans l'intérêt de la société. La police et le ministère public sont liés à cet égard à des dispositions légales bien définies. Cependant, la technique donne aussi à des personnes privées les moyens d'espionner des tiers de façon illégale. La forge de logiciels thaïlandaise Vervata par exemple a développé un petit programme qui fonctionne comme un cheval de Troie. Il fait d'un téléphone mobile un mini-espion et transmet même les conversations téléphoniques ou les bruits ambiants aux épieurs. Il suffit d'avoir en main le smartphone pendant quelques minutes pour installer le programme «Flexispy». Ce logiciel transmet les données à un serveur en Thaïlande auquel le fouinard peut se connecter pour relever les appels entrant et sortant: les numéros des destinataires et des appelants, y compris leurs noms dans le carnet d'adresses, la durée des communications et d'autres renseignements semblables. Le lieu où se trouve le propriétaire du téléphone mobile n'est pas caché au cheval de Troie: sur demande, celui-ci prend note du numéro de la station radio de base à laquelle le téléphone mobile vient de s'enregistrer. A l'origine, Flexispy a été développé pour prendre sur le fait des partenaires infidèles; aujourd'hui, le distributeur recommande ce programme en Allemagne aux parents qui veulent garder le contrôle sur le téléphone mobile de leurs enfants ou trouver leurs rejetons par le biais du signal GPS. Reste à espérer que le mariage de Salomé et Klemens tiendra longtemps et restera heureux – ou qu'au moins le couple ne recourra pas, s'il voulait se séparer, à des logiciels espions à la limite de la légalité.

Où suis-je – et où sont mes données ?

Dans les réseaux sociaux, les utilisateurs dévoilent une quantité de données qui parviennent éventuellement à des tiers par des voies peu transparentes. C'est ainsi que la directive de protection des données de Facebook relative aux lieux mentionne la possibilité pour cette organisation de fournir des informations sur le site de l'ordinateur ou dispositif d'accès de l'utilisateur ainsi que l'âge de ce dernier à des applications et sites web; la raison avancée est que ceux-ci doivent pouvoir prendre des mesures de sécurité adéquates et contrôler la diffusion de contenus adaptés à l'âge. A qui exactement Facebook transmet ces données et à quel usage? L'utilisateur ne reçoit pas d'informations précises à ce sujet. Il serait toutefois naïf de supposer que le fondateur de Facebook, Mark Zuckerberg, ait eu à l'esprit uniquement la protection des utilisateurs. L'intérêt des données récoltées tient bien plus à leur grande valeur pour le marketing de toutes sortes d'entreprises. Celles-ci paient gros pour avoir connaissance des données et messages des internautes: la société Gnip s'est spécialisée dans la collecte de données publiquement accessibles sur Facebook, Twitter et d'autres plates-formes et les revend à des fins de marketing. Qui souhaite lire la moitié de ce «gazouillis» doit débourser 360 000 dollars US.

Contrairement à des sociétés qui ont les moyens, les privés ont de grandes difficultés à obtenir des renseignements concernant même leur propre portefeuille de données. Max Schrems par exemple, un étudiant autrichien en droit, a dû lancer pour cela l'initiative «Europe vs Facebook» comme plate-forme pour porter plainte contre ce réseau social. Celui-ci avait en effet refusé de lui donner accès aux données récoltées à



son sujet. Une fois imprimé, le contenu du CD-ROM qu'il a finalement reçu remplissait 1222 pages et contenait même toutes les inscriptions que Schrems croyait avoir effacées.

L'iPhone, téléphone mobile culte, a lui aussi été touché par un scandale retentissant. On apprenait en avril 2011 que les iPhones et iPads qui opèrent avec le système d'exploitation iOS4 enregistraient les données de déplacement des appareils dans un fichier local du téléphone mobile. Les itinéraires de leurs utilisateurs pouvaient donc être reconstitués à partir de ces données. En Corée du Sud, pays dont les habitants sont pourtant très ouverts aux nouvelles techniques de communication, 26 000 personnes ont déposé plainte contre Apple.

3 Protéger ses données personnelles

Les moyens techniques de saisie et traitement des données ont pour conséquence le stockage de toujours plus d'informations personnelles. Dans ces conditions, il est pratiquement exclu de garder le contrôle de nos données – ceci même si la loi nous procure des moyens à cet effet. Et à vrai dire, les législations nationales sont très difficiles à mettre en œuvre et imposer dans l'internet planétaire.

Comme il ressort du quotidien des activités en ligne de la famille Christen, les nombreuses bases de données et plates-formes de communication sur internet permettent même à des personnes privées d'espionner la vie et les habitudes de tiers sans avoir aucune aptitude de hacker. Considérée superficiellement, cette manière de faire semble même être de droit: la Constitution fédérale de la Confédération suisse relève à l'article 16 sur les libertés d'opinion et d'information que toute personne «a le droit de recevoir librement des informations, de se les procurer aux sources généralement accessibles et de les diffuser». Et la loi suisse sur la protection des données confirme à la section 3 au sujet du traitement de données personnelles par des personnes privées qu'il n'y a «pas atteinte à la personnalité lorsque la personne concernée a rendu les données accessibles à tout un chacun et ne s'est pas opposée formellement au traitement». Il est toutefois incontesté parmi les juristes que les réseaux sociaux ne sont pas à considérer comme des plates-formes accessibles à tous. En effet, de nombreux éléments qui y figurent ne peuvent être lus que par les autres membres du réseau. De plus, les réseaux donnent à leurs utilisatrices et utilisateurs la possibilité de cacher leurs photos et envois à des étrangers.

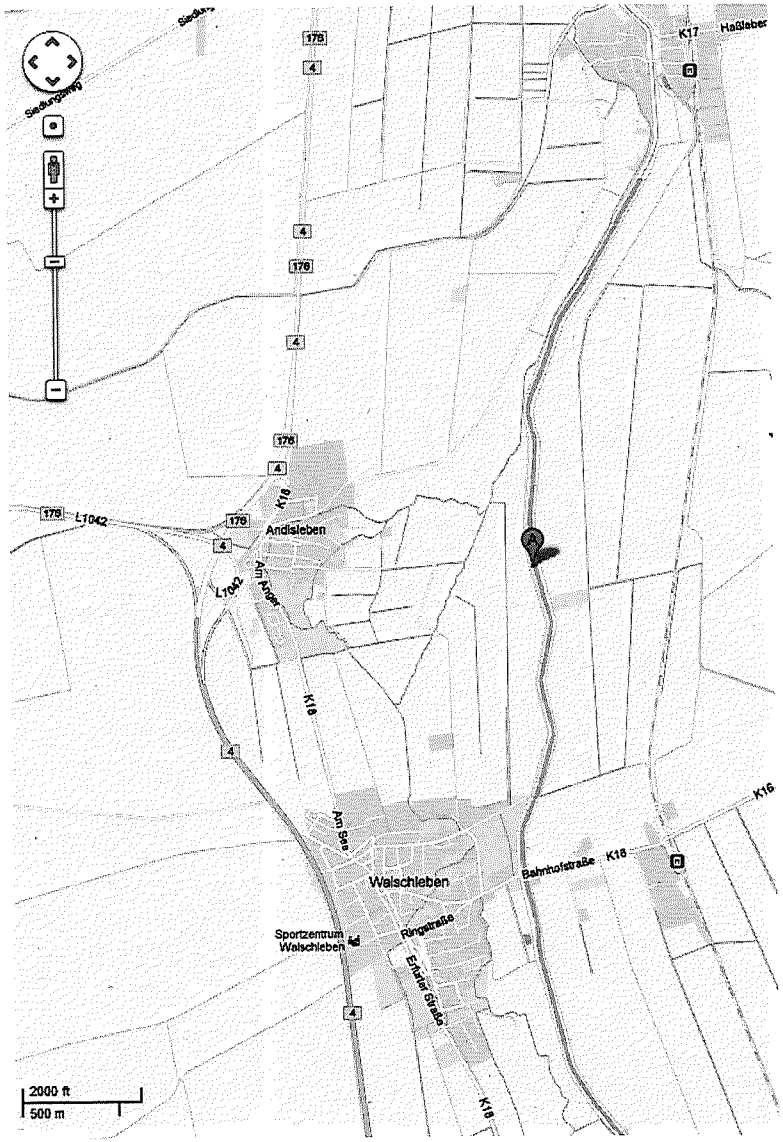
Mais les données géographiques de position sont-elles vraiment des informations personnelles? L'article 3 de la loi sur la protection des données laisse entendre que tel est le cas. Il définit les données personnelles comme «informations qui se rapportent à une personne identifiée ou identifiable». Dans cette optique, les données sur des itinéraires souvent parcourus peuvent révéler l'activité ou le domicile d'une personne et donc en fin de compte leur identité. Dans certains cas, les données géographiques de position peuvent même être considérées comme «données sensibles» – par exemple lorsque des photos qui ont été prises près d'une manifestation politique peuvent donner lieu à des spéculations sur les opinions de la personne en question.

Perte de contrôle garantie

Un gros problème réside dans la durée illimitée de conservation des informations publiées sur le web: de fait, les personnes qui bloguent et publient des photos des années durant perdent la vue d'ensemble sur leurs données. Que celles-ci puissent être arrachées de leur contexte et réapparaître plus tard à une autre place sur internet échappe dans une large mesure à leur contrôle.

Un aspect délicat est qu'il arrive que des tiers publient des informations et des images de leurs connaissances – comme cela s'est passé pour Salomé et Klemens avec la collection photographique de Patrick. Le couple lui-même reste discret dans ses propres blogs et téléchargements de photos. Les portraits par exemple que tous deux publient dans les réseaux sociaux ne montrent qu'une partie de leurs visages: une mèche de cheveux attachée derrière, un œil souriant, un piercing coquin.

Le problème ne cesse de s'aggraver avec le développement technique: des programmes de reconnaissance des visages sont apparus entre-temps qui scannent rapidement de grandes quantités de photos et les



classent en fonction de personnes qui y figurent. Les réseaux sociaux Google+ et Facebook ont déjà intégré des fonctions de ce genre à leur offre. La reconnaissance automatique des visages a fait des progrès considérables ces derniers temps, mais elle n'est pas encore toujours fiable. Pour les personnes concernées, une classification erronée de photos peut soulever des problèmes tout aussi graves qu'un profil correct et sans faille permettant de tirer des conclusions sur leur manière de vivre.

S'abstenir n'est pas non plus une solution

Quelqu'un peut superficiellement se protéger en refusant de publier des données personnelles sur des plates-formes d'information et de communication: qui reste à l'écart des réseaux sociaux n'y divulgue pas non plus de renseignements. Cependant, le refus de communiquer trahit aussi beaucoup de choses sur une personne et peut être interprété à son désavantage. Des responsables des ressources humaines, qui recherchent en vain dans les réseaux sociaux courants des informations sur un candidat convoqué à un entretien d'embauche, pourraient supposer que la personne en question a quelque chose à cacher ou qu'elle est pour le moins méfiante et peu apte à travailler en équipe. L'absence de traces sur internet peut donc même conduire à discriminer une personne.

A ceci s'ajoute que toujours plus de données de localisation sont collectées dans l'espace public – par exemple là où des caméras vidéo sont installées pour prévenir des actes criminels ou le vandalisme. Le seul moyen de se soustraire à une telle localisation est d'éviter les lieux placés ainsi sous surveillance; mais cela revient en fin de compte à amputer le droit fondamental à la liberté de mouvement, inscrit dans la Constitution fédérale.

Le détournement des objectifs est juridiquement discutable

Selon l'article 4 de la loi suisse sur la protection des données, qui énonce le principe fondamental de l'affectation des informations, «les données personnelles ne doivent être traitées que dans le but qui est indiqué lors de leur collecte, qui est prévu par une loi ou qui ressort des circonstances». Si l'on prend ce principe à la lettre, la plupart des réseaux sociaux agissent de façon discutable. Car l'utilisateur partage ses données pour entrer en relation avec ses «amis» et échanger des nouvelles; pour le non-initié, il ne ressort pas sans autres «des circonstances» que le principe commercial de la plate-forme repose sur la vente des données à des fins de marketing.

Il est vrai que dans leurs conditions générales, détaillées et pas toujours faciles à comprendre, Facebook et Cie. justifient la transmission de données en alléguant que les mineurs doivent être protégés et que l'offre d'informations de tiers doit être adaptée aux intérêts des utilisatrices et utilisateurs. En fait les réseaux sociaux posent comme condition que les utilisateurs renoncent à protéger les données touchant à leur personne. Les autorités de protection des données mettent pour le moins en doute que cette déclaration de consentement soit juridiquement valable. Et même si les utilisateurs font connaître le lieu où ils se trouvent dans le contexte d'autres applications, par exemple sur leur iPhone, ils ne donnent pas au destinataire la liberté d'utiliser ces données à leur guise.

Nombreuses lacunes au niveau de la mise en œuvre

En principe, la loi suisse sur la protection des données offre plusieurs moyens de se défendre aux personnes qui s'estiment victimes d'une violation de leur droit en la matière. Le demandeur peut requérir que le traitement de ses données soit interdit, que celles-ci ne soient plus communiquées à des tiers ou qu'elles soient rectifiées ou détruites. Mais la référence à une loi nationale de protection des données n'est guère en mesure d'impressionner un fournisseur de services opérant à l'échelle internationale tel que Facebook ou Google; Max Schrems (voir l'encadré à la page 9) n'est parvenu à motiver le réseau social à lui remettre les informations le concernant qu'après avoir lancé une initiative efficace auprès du public et obtenu le soutien de l'autorité irlandaise, responsable dans ce cas précis – le siège européen de Google se trouve à Dublin – de la protection des données en Europe. La menace d'une atteinte à son image n'a probablement pas eu moins de poids que les arguments juridiques pour inciter Facebook à se montrer conciliant.

En fait, c'est souvent le souhait de discrétion qui retient les personnes concernées à se défendre contre les violations des droits de la personnalité et à insister pour obtenir la protection de leurs données. Car des démêlés juridiques impliquent parfois que le demandeur doive divulguer des informations qu'il préférerait taire et les rendre accessibles à de plus larges cercles que cela ne serait le cas sans litige.

La globalisation des communications nécessite une protection mondiale

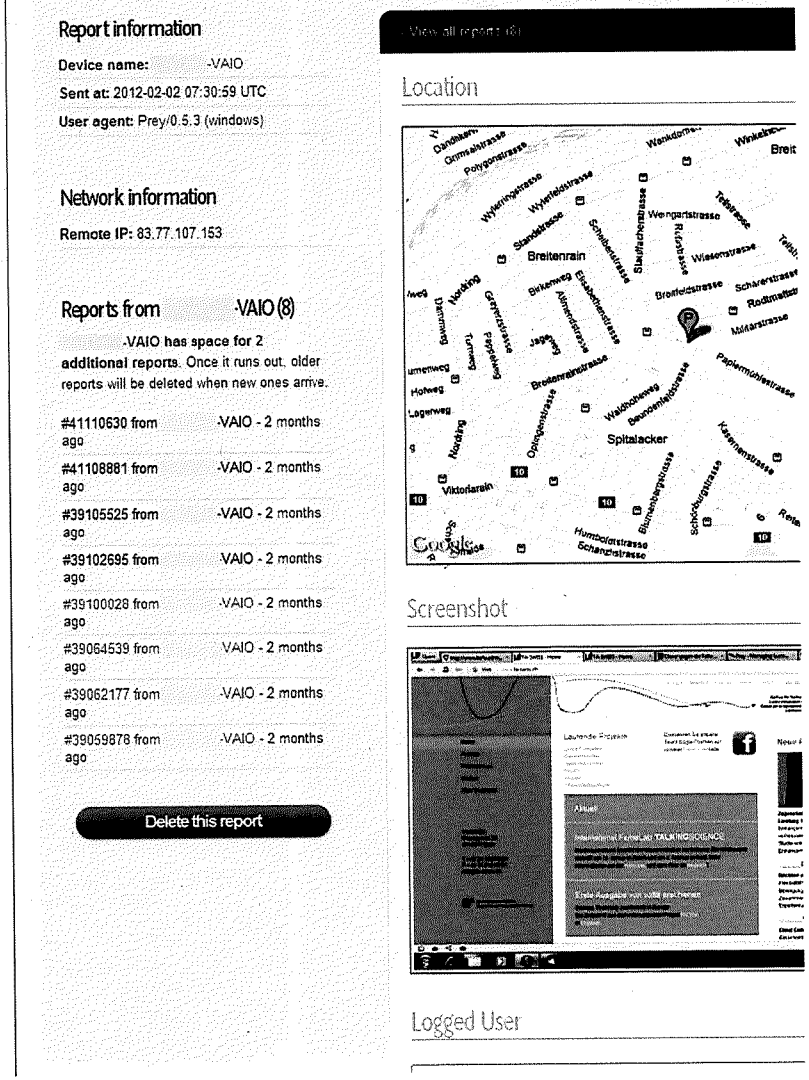
Dans quelle mesure la loi suisse de protection des données est-elle applicable à la saisie de données par un fournisseur de services agissant à l'étranger? La question fait apparaître de nombreux points à éclaircir. Les juristes partent de l'idée que le Préposé fédéral à la protection des données et à la transparence (PFPDT) peut intervenir si des données sont traitées en Suisse même. Mais dans quelle mesure cette condition est satisfaite pour des réseaux sociaux opérant depuis l'étranger est pour le moins controversé parmi les

juristes. Dans les litiges internationaux, il faut de plus clarifier les compétences.

Des efforts sont en cours actuellement au niveau européen pour renforcer la protection des données. La Commission européenne critique notamment que les renseignements sur la protection des données publiés dans les environnements en ligne sont souvent peu clairs, difficiles à trouver et peu transparents. Elle exige en outre une amélioration des droits de contrôle à disposition des personnes concernées par le traitement de leurs données. A propos des indications révélant la position géographique, un organe consultatif de la Commission européenne recommande que les services de localisation soient nécessairement inactifs dans le réglage standard. Il faudrait en outre que les personnes ayant consenti à l'utilisation de «leurs» données de localisation doivent renouveler leur consentement chaque année et puissent l'annuler facilement. Les fournisseurs devraient être tenus d'afficher un avertissement permanent pour les fonctionnalités de localisation dont l'utilisateur n'a pas conscience.

En vertu des accords d'association de Schengen/Dublin, la Suisse a l'obligation d'appliquer plusieurs actes juridiques de l'UE ayant trait au droit de la protection des données. Les modifications du droit européen prévues en raison des nouvelles possibilités techniques seraient donc aussi valables pour la Suisse. Cela signifierait qu'en Suisse également les personnes concernées verraient leurs droits de protection renforcés quant au traitement de leurs données – une telle évolution trouverait sans doute aussi l'approbation de Salomé et Klemens. La discrétion qu'ils observent dans les réglages de leurs comptes de réseaux, en ne rendant visible qu'à des amis leur adresse privée et numéro de téléphone, permet en tous cas de conclure qu'ils ont à cœur de protéger leurs données personnelles.

L'internet vit de l'actualisation permanente et rapide de ses contenus. Les réseaux sociaux aussi adaptent constamment leurs offres et modifient alors souvent les masques des formulaires à remplir pour déterminer qui peut voir quelles informations. Des conseils de réglages pour améliorer la protection de la sphère privée et la sûreté de la communication sur le web se trouvent par exemple sous:
www.datenschutz.ch
www.bsi-fuer-buerger.de
www.cnpd.public.lu (Commission nationale pour la protection des données du Grand-Duché de Luxembourg)
www.europe-v-facebook.org/FR/fr.html



Etude «Lokalisiert und identifiziert. Wie Ortungstechnologien unser Leben verändern»

Groupe d'accompagnement

- Dr. Bruno Baeriswyl, Préposé cantonal à la protection des données, Zurich; Comité directeur de TA-SWISS (Président du groupe d'accompagnement)
- Florence Bettschart, Fédération romande des consommateurs (FRC), Lausanne
- Alain Buogo, Office fédéral de topographie swisstopo, Wabern
- Dr. Christine Giger, Giger GeoIT, Embrach
- Prof. Dr. Gudela Grote, Psychologie industrielle et organisationnelle, EPFZ, Zurich
- Dr. Jessica Heesen, Université Eberhard Karls, Tübingen
- Rainer Humbel, Office fédéral de la statistique OFS, Neuchâtel
- Thomas Kallweit, FELA Management AG, Diessenhofen
- Dr. Francisco Klauser, Institut de géographie, Université de Neuchâtel, Neuchâtel
- Michael Kocheisen, Swisscom Innovation Competence Center, Swisscom (Suisse) SA, Berne
- Ulrich Lattmann, Académie suisse des sciences techniques ASST, Zurich
- Urs Luther, Office fédéral des routes OFROU, Berne
- Franziska Meister, Die Wochenzeitung, Zurich
- Cyrill Osterwalder, Google, Zurich
- Hans Kaspar Schiesser, Association des transports publics, Berne
- Philipp Stüssi, Service du Préposé fédéral à la protection des données, Berne
- Prof. Dr. Rolf H. Weber, Centre de droit de l'information et de la communication, Université de Zurich, Zurich
- Dr. Franz Zeller, Office fédéral de la communication OFCOM, Bienne

Responsables de projets

- Dr. Sergio Bellucci, TA-SWISS, Berne
- Nadia Ben Zbir, TA-SWISS, Berne

Impressum

TA-SWISS (éd). Repères géographiques dans le cybermonde. Le défi des technologies de localisation pour une société ouverte.

Résumé de l'étude de TA-SWISS «Lokalisiert und identifiziert. Wie Ortungstechnologien unser Leben verändern», Berne 2012.

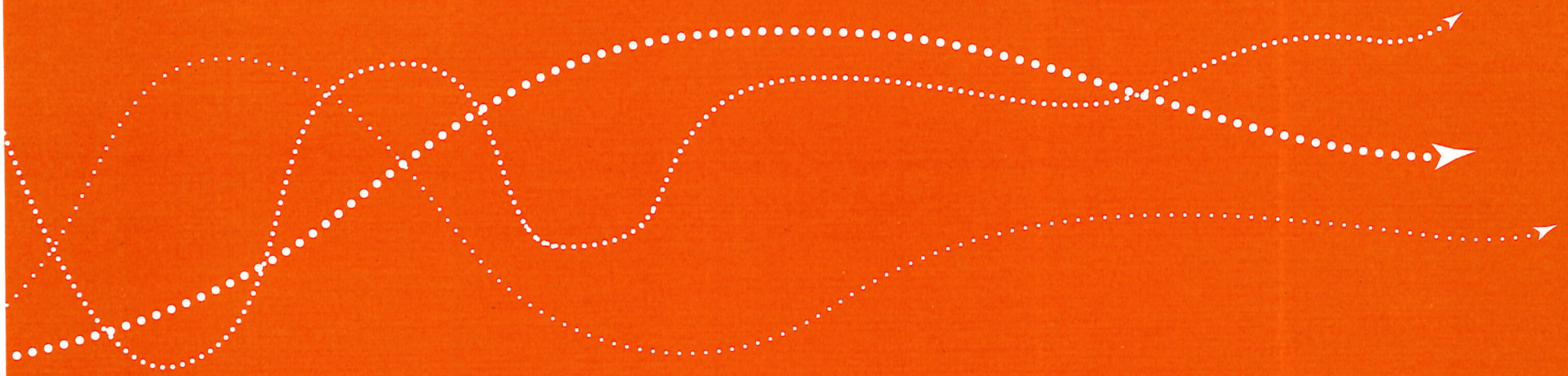
TA 57A/2012

Auteur : Lucienne Rey, Berne
Rédaction : Christine D'Anna-Huber, TA-SWISS
Traducteur : Jean-Jacques Daetwyler, Berne
Mise en pages: Hannes Saxer, Berne
Photos : Lucienne Rey
Impression: Jordi AG – Das Medienhaus, CH-3123 Belp

TA-SWISS – Le Centre d'évaluation des choix technologiques

Souvent susceptibles d'avoir une influence décisive sur la qualité de vie des gens, les nouvelles technologies peuvent en même temps comporter des risques nouveaux, qu'il est parfois difficile de percevoir d'emblée. Le Centre d'évaluation des choix technologiques TA-SWISS s'intéresse aux avantages et aux risques potentiels des nouvelles technologies qui se développent dans les domaines «biotechnologie et médecine», «société de l'information», «nanotechnologies» et «mobilité/énergie/climat». Ses études s'adressent tant aux décideurs du monde politique et économique qu'à l'opinion publique. TA-SWISS s'attache, en outre, à favoriser par des méthodes dites participatives, telles que les PubliForums et publifocus, l'échange d'informations et d'opinions entre les spécialistes du monde scientifique, économique et politique et la population. TA-SWISS se doit, dans toutes ses projets sur les avantages et les risques potentiels des nouvelles technologies, de fournir des informations aussi factuelles, indépendantes et étayées que possible. Il y parvient en mettant chaque fois sur pied un groupe d'accompagnement composé d'experts choisis de manière à ce que leurs compétences respectives couvrent ensemble la plupart des aspects du sujet à traiter.

TA-SWISS est rattaché aux Académies suisses des sciences



Centre d'évaluation des choix technologiques
Brunngasse 36
CH-3011 Berne
info@ta-swiss.ch
www.ta-swiss.ch

Un centre de compétence des
Académies suisses des sciences

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Office fédéral des routes OFROU

Office fédéral de la statistique OFS

Office fédéral de topographie swisstopo